AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* information associated with banmeet.pay@gmail.com that is stored at the premises controlled by GOOGLE	)	Case No. 2:17mj734 MAGISTRATE JUDGE JOLSON

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A, which is attached hereto and incorporated herein by reference

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B, which is attached hereto and incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 959	Manufacture or Distribution of MDMA for the Purpose of Unlawful Importation

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew Wuertz, DEA Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: Dec 6, 2017

Judge's signature

City and state: Columbus, OH

Kimberly A. Jolson, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH banmeet.pay@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE

Case No. 2:17mj734

Filed Under Seal

MAGISTRATE JUDGE JOLSON

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Task Force Officer Andrew Wuertz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by GOOGLE, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require GOOGLE to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am currently employed as a Detective by the City of Upper Arlington Division of Police, and I have concurrently been serving as a Task Force Officer with the Drug Enforcement Administration (hereinafter referred to as "DEA") since June of 2010. Being duly appointed according to law and acting as such, I am an investigative or law

enforcement officer within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in 18 U.S.C. § 2516. In that capacity, I have participated in investigations involving the debriefing of illegal narcotics traffickers, review of electronic information obtained pursuant to search warrants issued to electronic communications providers, review of telephone records and GPS data, review of money transfer records, surveillance, analysis of pen register information, review of electronically stored communications, and various other investigative techniques. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities, to communicate with co-conspirators known and unknown, and to arrange for the transport of contraband, including narcotics.

3. The facts in this affidavit come from my personal observations, my training and experience, as well as my review of documents and information obtained from other law enforcement personnel and witnesses. Because the purpose of this affidavit is limited to demonstrating probable cause for the requested warrant, it does not set forth all of my knowledge about this matter. In addition, when I rely on statements made by others, such statements are set forth only in part and in sum and substance unless otherwise indicated.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 959 have been committed by Banmeet SINGH, aka "LISTON", and his co-conspirators. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. In February of 2017, members of the DEA Columbus District Office initiated an investigation into the illegal narcotics trafficking activities of an individual later identified as Banmeet SINGH aka-LISTON. Based upon investigative efforts to date, as well as information obtained from preceding linked investigations, law enforcement has learned that SINGH, an India national, is situated at the head of a drug trafficking organization (DTO) responsible for the shipment of kilogram-quantity shipments of MDMA, Ketamine, and other illegal narcotics from Europe to customers located throughout the United States, and other foreign countries. Portions of the illegal narcotics shipments have arrived in the Southern District of Ohio for distribution, or transit from the Southern District of Ohio enroute to other distribution locations in the United States.

7. In January 2017, the Agents from the Drug Enforcement Administration (DEA), in Ashville, North Carolina identified a local target who was utilizing the "dark web" and the United States Postal Service (USPS), to anonymously obtain and distribute MDMA and other controlled substances throughout the United States and internationally. The investigation revealed that from October 2015 through December 2016, this local target, identified as Amanda TRULL, shipped over 4,200 packages of suspected controlled

substances to over 2,500 different addresses within the continental United States, the U.S. Virgin Islands, and internationally to Canada, Jamaica and Ireland. The investigation identified two sources of supply for TRULL; one in the Baltimore, MD and the other on Staten Island, New York. Agents from DEA Ashville learned the Baltimore source has also received parcels from various European countries.

8. On January 19, 2017, DEA Ashville, working in conjunction with Inspectors from the USPS conducted a search warrant at Amanda TRULL's residence. The basis for the search warrant was the result of a trash pull from TRULL's residence that yielded two and a half (2.5) pounds of MDMA dust she had thrown away. During the search of her residence Agents seized approximately 59 kilograms of MDMA, approximately 14 kilograms of Ketamine, three (3) ounces of Heroin, and an assortment of Schedule IV controlled substances.

9. TRULL cooperated with Agents and stated that after being asked by a friend (identified as Benjamin ROTEN), if she wanted to make extra money shipping packages, ROTEN put her in contact with a person only known to her as LISTON. TRULL explained she would receive packages from Europe, New York, New Jersey, Florida, and other states, and would communicate with LISTON using the Wickr encrypted app, and through email on where to ship the contents of the boxes. When TRULL received packages she always found them to contain MDMA, Ketamine, and other illegal narcotics. TRULL was aware LISTON was a retail seller of illegal drugs on the "dark web".

10. On March 1, 2017, agents with the New York Organized Crime Drug Enforcement Strike Force (NYOCDESF), Group Z-51, conducted a controlled delivery of

approximately four and a half (4.5) kilograms of MDMA tablets to Anthony CORONATI at his address in Staten Island, NY. During his post arrest interview after being Mirandized CORONATI told agents he initially started communicating with an individual via email after requesting to purchase steroids online via a steroid forum. The email the individual used in communicating with CORONATI was listonishere@gmail.com. CORONATI stated that after an unspecified time of purchasing steroids, he received a package containing an unknown type of pills. CORONATI contacted LISTONISHERE using the listonishere@gmail.com email account, and was told the shipment was a mistake. LISTONISHERE replied via the listonishere@gmail.com email account and asked CORONATI to reship the package in return CORONATI would be paid cash. At this time CORONATI was asked by LISTONISHERE to communicate via Wickr. CORONATI stated the moniker LISTONISHERE used on Wickr was GANNICUSK (AKA- GANNICUS). CORONATI told agents that he started reshipping three to four (3-4) packages a week after the initial incident. CORONATI was paid approximately $800-$1400 to ship each package, and was paid with cash via mail or PayPal. CORONATI received the shipping instructions from LISTONISHERE (GANNICUSK) via Wickr. CORONATI generally received three to four (3-4) packages per week from international addresses, but said he only reshipped packages within the United States. CORONATI would confirm receipt of each package before receiving directions on where and how to ship each package from LISTONISHERE (GANNICUSK). CORONATI showed agents Wickr messages between himself and LISTONISHERE (GANNICUSK). It was also revealed that CORONATI was reshipping packages to TRULL.

11. Agents have since definitively linked the 'dark web' moniker LISTONISHERE to Banmeet SINGH, as well as determining the email addresses

listonishere@gmail.com, banmeet.elvis@gmail.com, indiabenzos@gmail.com, cadycailin321@gmail.com, aoberoi715@gmail.com, listonisheresales@gmail.com, shutupbannu@gmail.com, niceharvinder@gmail.com, aka.Parvinder@gmail.com, banmeet.pay@gmail.com, bsingh.elvis@gmail.com, antiliaproperties@gmail.com, antiliadental@gmail.com, Bitoworld.ltd@gmail.com, Akc4bsn@gmail.com, dr.amarpreet86@gmail.com, listonpharma@gmail.com, agniashu@gmail.com, and badgerscrote9@gmail.com are either controlled by, or associated with, SINGH. SINGH uses these emails to facilitate his drug trafficking activity on the 'dark web' as well as to communicate with others in an attempt to evade law enforcement. ****

12. Summary of Probable Cause ----- Banmeet SINGH aka-LISTON aka-LISTONISHERE has been identified as a large-scale distributor of MDMA, Ketamine and other illegal narcotics. SINGH primarily uses the 'dark web' to conduct his trafficking activities and enlists several "re-shippers" to send narcotics to hundreds of customers throughout the U.S. and internationally. DEA Columbus and their law enforcement partners have intercepted several such packages as described earlier in this affidavit as well as cultivated cooperating witnesses. Through these and other investigative techniques your affiant has associated the following email addresses listonishere@gmail.com, banmeet.elvis@gmail.com , indiabenzos@gmail.com, cadycailin321@gmail.comaoberoi715@gmail.com, listonisheresales@gmail.com, shutupbannu@gmail.com, niceharvinder@gmail.com, aka.Parvinder@gmail.com, banmeet.pay@gmail.com, bsingh.elvis@gmail.com, antiliaproperties@gmail.com, antiliadental@gmail.com, Bitoworld.ltd@gmail.com, Akc4bsn@gmail.com, dr.amarpreet86@gmail.com, listonpharma@gmail.com, agniashu@gmail.com, and

badgerscrote9@gmail.com as being controlled by, or associated with, LISTON's narcotics trafficking activities on the 'dark web'.

13. On December 5, 2017, a preservation request was served upon GOOGLE, thereby ensuring the evidence sought remains in the care and control of GOOGLE. In general, an email that is sent to a GOOGLE subscriber is stored in the subscriber's "mail box" on GOOGLE servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on GOOGLE servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on GOOGLE's servers for a certain period of time.

14. On December 5, 2017, GOOGLE confirmed via responsive email the preservation of the evidence being sought, storing the responsive evidence under Reference Number 1321161.

BACKGROUND CONCERNING EMAIL

15. In my training and experience, I have learned that GOOGLE provides a variety of online services, including electronic mail ("email") access, to the public. GOOGLE allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with GOOGLE. During the registration process, GOOGLE asks subscribers to provide basic personal information. Therefore, the computers of GOOGLE are likely to contain stored electronic communications (including retrieved and unretrieved email for GOOGLE subscribers) and information concerning subscribers and their use of GOOGLE services, such as account access

information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

17. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the

Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

18. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. This application seeks a warrant to search all responsive records and information under the control of GOOGLE, a provider subject to the jurisdiction of this court, regardless of where GOOGLE has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within GOOGLE's possession, custody, or control, regardless of whether such communication, record, or other

information is stored, held, or maintained outside the United States. [1]

20. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and

[1] It is possible that GOOGLE stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of GOOGLE. However, I am mindful of the Court's previous decision that a request for information stored, held, or maintained outside of the United States is premature at this time because the location(s) where the GOOGLE stores, holds, or maintains the responsive information sought by this warrant is unknown at the present time. Accordingly, the government also seeks the disclosure of the physical location or locations where the information is stored. the government requests that the Court order, via Attachment B, that the GOOGLE disclose in writing to the government the physical location(s) where the responsive information is stored, held, and/or maintained, whether inside or outside of the United States.

timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

21. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on GOOGLE, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR NON-DISCLOSURE AND SEALING

22. The United States request that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), GOOGLE be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this warrant would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and/or flee from prosecution.

23. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and/or flee from prosecution.

Respectfully submitted,

Andrew Wuertz
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me on Dec 6, 2017

Honorable Kimberly A. Jolson
UNITED STATES MAGISTRATE JUDGE